UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/992,582	11/16/2001	Stephen M. Hitchen	1152-2U	8250

29973 7590 03/02/2009

CAREY, RODRIGUEZ, GREENBERG & PAUL LLP
ATTN: STEVEN M. GREENBERG, ESQ.
950 PENINSULA CORPORATE CIRCLE
SUITE 3020
BOCA RATON, FL 33487

EXAMINER	
WASSUM, LUKE S	

ART UNIT	PAPER NUMBER
2167	

MAIL DATE	DELIVERY MODE
03/02/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	09/992,582	HITCHEN ET AL.	
	Examiner	Art Unit	
	Luke S. Wassum	2167	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *12 December 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-8 and 12-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-8 and 12-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *16 November 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Prosecution Reopened

1. In view of the Decision of the Board of Patent Appeals and Interferences, rendered on 12 December 2008, and newly discovered prior art, new grounds of rejection based upon prior art not previously of record are presented herein.

PROSECUTION IS HEREBY REOPENED.

2. A technology Center Director or designee has approved the reopening of prosecution by signing below:

/ANDREW H HIRSHFELD/
Director, TC 2100

Response to Amendment

3. The Applicants' amendment, filed 12 December 2008, has been received, entered into the record, and considered.

4. As a result of the amendment, claims 9-11 have been canceled. Claims 1-8 and 12-20 remain pending in the application.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. The factual inquiries set forth in *Graham* v. *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

7. This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to

consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

8. Claims 1-8 and 12-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Ginter et al.** (U.S. Patent 5,910,987) in view of **McCurdy et al.** (U.S. Patent Application Publication 2002/0035697) in view of **Graham et al.** (U.S. Patent Application Publication 2002/0178271).

9. Regarding claim 1, **Ginter et al.** teaches a collaborative file rights management method as claimed, comprising:

a) identifying a file input/output (I/O) request to access a file, said file I/O request originating in an authoring application (see disclosure of the events process that detects events, for instance, a request from a user to access content, col. 55, lines 53-61 et seq.; see also disclosure that the system can be used by content authors, inter alia, col. 11, lines 40-50 et seq.);

b) automatically extracting digital rights management data appended to said file (see disclosure that when a user who lacks permission requests access to

content, the request will be denied, col. 55, lines 60-61; see also disclosure that container 302 contains content as well as the contents' associated permissions record, col. 56, lines 52-65, as well as drawing Figures 5A and 5B; see also disclosure of 'traveling objects', whereby objects are distributed with permissions records embedded therein, thus allowing use of the object at any VDE appliance/participant, col. 128, lines 38-60; these three disclosures rendering the claimed extraction of digital rights management data appended to said file inherent, since the permissions data is included within the content container, and the permissions information is required by the event process to determine whether a specific user request will be granted or denied); and

c) providing said file to said authoring application (see disclosure of the granting of a user's request for access to content, col. 55, lines 53-67 et seq.; see also disclosure that the system can be used by content authors, inter alia, col. 11, lines 40-50 et seq.).

Ginter et al. does not explicitly teach a collaborative file rights management method including the step of managing access to said file in said authoring application based upon said extracted digital rights management data.

McCurdy et al., however, teaches a collaborative file rights management method including managing access to said file in said authoring application based upon said extracted digital rights management data (see paragraphs [0137] through [0140]).

It would have been obvious to one of ordinary skill in the art at the time of the invention to perform the claimed intercepting, detecting and quashing steps in cooperation with an authoring application, since digital rights management dictates that users with no rights to individual parts of a document be prohibited from copying not only an entire document, but the individual protected parts (see paragraphs [0137] and [0138]).

Neither **Ginter et al.** nor **McCurdy et al.** explicitly reaches suppressing said file I/O request.

Graham et al., however, teaches a system which provides selective access and usage management to files available from one or more file systems or sources (see paragraph [0011]) through the use of a filter driver, wherein a request dispatched to the file system is intercepted and suppressed by the filter driver, and wherein the filter

driver interfaces with the file system and adds additional functionality beyond that offered by the existing file system (see paragraphs [0140] and [0141]).

It would have been obvious to one of ordinary skill in the art at the time of the invention to intercept and suppress file I/O requests in order to implement usage management, since this allows clients to access and utilize files without changing the process for accessing files in any way from the user's perspective, i.e., users continue to use Network Neighborhood or content management software, and other standard applications to access remote storage drives and directories (see paragraphs [0138] and [0139]).

10. Regarding claim 12, **Ginter et al.** teaches a collaborative file rights management system as claimed, comprising:

a) a file security management application configured to intercept operating system messages directed to an authoring application (see disclosure of the events process that detects events, for instance, a request from a user to access content, col. 55, lines 53-61 et seq.; see also disclosure that the system can be used by content authors, inter alia, col. 11, lines 40-50 et seq.); and

b) said file security management application extracting digital rights management data appended to said file, detecting among intercepted operating system messages operating system messages directed to authoring applications which can be limited according to digital rights specified in said extracted digital rights management data and quashing said detected events where said digital rights management data prohibits execution of said authoring application operations (see disclosure that when a user who lacks permission requests access to content, the request will be denied, col. 55, lines 60-61; see also disclosure that container 302 contains content as well as the contents' associated permissions record, col. 56, lines 52-65, as well as drawing Figures 5A and 5B; see also disclosure of 'traveling objects', whereby objects are distributed with permissions records embedded therein, thus allowing use of the object at any VDE appliance/participant, col. 128, lines 38-60; these three disclosures rendering the claimed extraction of digital rights management data appended to said file inherent, since the permissions data is included within the content container, and the permissions information is required by the event process to determine whether a specific user request will be granted or denied).

Ginter et al. does not explicitly teach a collaborative file rights management system including the automatic encryption and decryption of the file.

McCurdy et al., however, teaches a collaborative file rights management method further comprising automatically encrypting said file (see paragraph [0016]) and decrypting said file (see paragraph [0205].

It would have been obvious to one of ordinary skill in the art at the time of the invention to automatically decrypt a retrieved file, since encryption/decryption is a well known and widely used technique for protecting data and/or files from access by unauthorized users, and decryption is necessary for an authorized user to access an encrypted file.

Neither **Ginter et al.** nor **McCurdy et al.** explicitly teaches a file security filter driver configured to identify file input/output (I/O) requests received in a kernel-layer system manager to open a file in said authoring application, said file security driver providing said file to said authoring application.

Graham et al., however, teaches a system which provides selective access and usage management to files available from one or more file systems or sources (see paragraph [0011]) through the use of a filter driver, wherein a request dispatched to the file system is intercepted and suppressed by the filter driver (see paragraphs [0140] and [0141]), and wherein the filter driver interfaces with the file system and adds additional functionality beyond that offered by the existing file system in order to enforce usage policies and based on said usage policies, either providing the requested file or denying the request (see paragraphs [0119], [0125] and [0131]).

It would have been obvious to one of ordinary skill in the art at the time of the invention to intercept and suppress file I/O requests in order to implement usage management, since this allows clients to access and utilize files without changing the process for accessing files in any way from the user's perspective, i.e., users continue to use Network Neighborhood or content management software, and other standard applications to access remote storage drives and directories (see paragraphs [0138] and [0139]).

11. Regarding claim 13, **Ginter et al.** teaches a machine readable storage having stored thereon a computer program for managing digital rights in a collaborative file, said computer program comprising a routine set of instructions for causing the machine to perform the steps of:

a) identifying a file input/output (I/O) request to access a file, said file I/O request originating in an authoring application (see disclosure of the events process that detects events, for instance, a request from a user to access content, col. 55, lines 53-61 et seq.; see also disclosure that the system can be used by content authors, inter alia, col. 11, lines 40-50 et seq.);

b) automatically extracting digital rights management data appended to said file (see disclosure that when a user who lacks permission requests access to content, the request will be denied, col. 55, lines 60-61; see also disclosure that container 302 contains content as well as the contents' associated permissions record, col. 56, lines 52-65, as well as drawing Figures 5A and 5B; see also disclosure of 'traveling objects', whereby objects are distributed with permissions records embedded therein, thus allowing use of the object at any VDE appliance/participant, col. 128, lines 38-60; these three disclosures rendering the claimed extraction of digital rights management data appended to said file inherent, since the permissions data is included

within the content container, and the permissions information is required by the event process to determine whether a specific user request will be granted or denied); and

c) providing said file to said authoring application (see disclosure of the granting of a user's request for access to content, col. 55, lines 53-67 et seq.; see also disclosure that the system can be used by content authors, inter alia, col. 11, lines 40-50 et seq.).

Ginter et al. does not explicitly teach a computer program for managing digital rights including the step of managing access to said file in said authoring application based upon said extracted digital rights management data.

McCurdy et al., however, teaches a computer program for managing digital rights including managing access to said file in said authoring application based upon said extracted digital rights management data (see paragraphs [0137] through [0140]).

It would have been obvious to one of ordinary skill in the art at the time of the invention to perform the claimed intercepting, detecting and quashing steps in cooperation with an authoring application, since digital rights management dictates

that users with no rights to individual parts of a document be prohibited from copying not only an entire document, but the individual protected parts (see paragraphs [0137] and [0138]).

Neither **Ginter et al.** nor **McCurdy et al.** explicitly reaches suppressing said file I/O request.

Graham et al., however, teaches a system which provides selective access and usage management to files available from one or more file systems or sources (see paragraph [0011]) through the use of a filter driver, wherein a request dispatched to the file system is intercepted and suppressed by the filter driver, and wherein the filter driver interfaces with the file system and adds additional functionality beyond that offered by the existing file system (see paragraphs [0140] and [0141]).

It would have been obvious to one of ordinary skill in the art at the time of the invention to intercept and suppress file I/O requests in order to implement usage management, since this allows clients to access and utilize files without changing the process for accessing files in any way from the user's perspective, i.e., users continue to use Network Neighborhood or content management software, and other standard

applications to access remote storage drives and directories (see paragraphs [0138] and [0139]).

12. Regarding claims 2 and 14, **McCurdy et al.**, however, teaches a collaborative file rights management method and computer program for managing digital rights further comprising decrypting said file (see paragraph [0205].

It would have been obvious to one of ordinary skill in the art at the time of the invention to automatically decrypt a retrieved file, since encryption/decryption is a well known and widely used technique for protecting data and/or files from access by unauthorized users, and decryption is necessary for an authorized user to access an encrypted file.

13. Regarding claims 3 and 15, **Ginter et al.** additionally teaches a collaborative file rights management method and computer program for managing digital rights wherein said extracting step further comprises:

a) determining environmental data associated with said I/O request, said environmental data comprising at least one of a requestor's identity, a

requestor's class, a requestor's computing domain, a requestor's location, a password, a time of day, and a date (see registration of the requestor's identity, col. 7, lines 16-21; see also col. 7, lines 35-46); and

b) extracting an access policy appended to said file (see disclosure that when a user who lacks permission requests access to content, the request will be denied, col. 55, lines 60-61; see also disclosure that container 302 contains content as well as the contents' associated permissions record, col. 56, lines 52-65, as well as drawing Figures 5A and 5B; see also disclosure of 'traveling objects', whereby objects are distributed with permissions records embedded therein, thus allowing use of the object at any VDE appliance/participant, col. 128, lines 38-60; these three disclosures rendering the claimed extraction of access policy appended to said file inherent, since the permissions data is included within the content container, and the permissions information is required by the event process to determine whether a specific user request will be granted or denied).

14. Regarding claims 4 and 16, **Ginter et al.** additionally teaches a collaborative file rights management method and computer program for managing digital rights wherein said providing step further comprises:

a) comparing said access policy to at least a portion of said environmental data (see disclosure that the "rules and controls" may grant specific individuals or classes of content users "permission" to use certain content, col. 54, lines 22-49; see also disclosure of the use of object data, user data, and rights data in determining whether a user request is fulfilled, col. 110, line 63 through col. 111, line 40);

b) authenticating said file I/O request based upon said comparison (see disclosure that the "rules and controls" may grant specific individuals or classes of content users "permission" to use certain content, col. 54, lines 22-49; see also disclosure of the use of object data, user data, and rights data in determining whether a user request is fulfilled, col. 110, line 63 through col. 111, line 40); and

c) providing said file to said authoring application only if said I/O request has been authenticated (see disclosure that the "rules and controls" may grant specific individuals or classes of content users "permission" to use certain content, col. 54, lines 22-49; see also disclosure of the use of object data, user data, and rights data in determining whether a user request is fulfilled, col. 110, line 63 through col. 111, line 40).

15. Regarding claims 5 and 17, **Ginter et al.** additionally teaches a collaborative file rights management method and computer program for managing digital rights wherein said suppressing step further comprises:

a) posting a responsive message to said authoring application (see disclosure that a user who lacks permission to access requested content will have their request denied, col. 55, lines 60-61); and

b) intercepting an operating system event in said authoring application, said operating system event indicating receipt of said responsive message (see disclosure that a user who lacks permission to access requested content will have their request denied, col. 55, lines 60-61).

Graham et al. additionally teaches quashing further processing of said intercepted operating system event (see disclosure that file I/O requests are intercepted through the use of a filter driver, wherein a request dispatched to the file system is intercepted and suppressed by the filter driver, and wherein the filter driver interfaces with the file system and adds additional functionality beyond that offered by the existing file system (see paragraphs [0140] and [0141]).

16. Regarding claims 6 and 18, **Graham et al.** additionally teaches a collaborative file rights management method and computer program for managing digital rights wherein said identifying step comprises:

a) monitoring kernel-level file I/O requests contained in I/O request packets processed in a file system manager (see disclosure that the client module identifies and intercepts calls between an application and the OS, paragraph [0119]); and

b) detecting said file I/O request to access said file in one of said I/O request packets (see disclosure that the client module identifies and intercepts calls between an application and the OS, paragraph [0119]).

It would have been obvious to one of ordinary skill in the art at the time of the invention to monitor and detect kernel-level I/O requests in order to implement usage management, since this allows clients to access and utilize files without changing the process for accessing files in any way from the user's perspective, i.e., users continue to use Network Neighborhood or content management software, and other standard applications to access remote storage drives and directories (see paragraphs [0138] and [0139]).

17. Regarding claims 7, 8, 19 and 20, **Ginter et al.** teaches a collaborative file rights management method and computer program for managing digital rights substantially as claimed.

Ginter et al. does not explicitly teach a collaborative file rights management method and computer program for managing digital rights wherein said management step comprises the claimed intercepting, detecting and quashing steps in cooperation with an authoring application wherein the protected operations are selected from clipboard operations, printing operations, file saving operations and file editing operations.

McCurdy et al., however, teaches a collaborative file rights management method and computer program for managing digital rights wherein said management step comprises:

a) intercepting operating system messages in said authoring application (see paragraphs [0137] through [0140]); and

b) detecting among said intercepted operating system messages, operating system messages directed to authoring application operations which can be limited according to digital rights specified in said extracted digital rights

management data, wherein the protected operations are selected from clipboard operations, printing operations, file saving operations and file editing operations (see paragraphs [0137] through [0140]).

Graham et al. additionally teaches quashing further processing of said intercepted operating system event (see disclosure that file I/O requests are intercepted through the use of a filter driver, wherein a request dispatched to the file system is intercepted and suppressed by the filter driver, and wherein the filter driver interfaces with the file system and adds additional functionality beyond that offered by the existing file system (see paragraphs [0140] and [0141]).

It would have been obvious to one of ordinary skill in the art at the time of the invention to perform the claimed intercepting, detecting and quashing steps in cooperation with an authoring application, since digital rights management dictates that users with no rights to individual parts of a document be prohibited from copying not only an entire document, but the individual protected parts (see paragraphs [0137] and [0138]).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Luke S. Wassum whose telephone number is 571-272-4119. The examiner can normally be reached on Monday-Friday 8:30-5:30, alternate Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, John R. Cottingham can be reached on 571-272-7079. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

In addition, INFORMAL or DRAFT communications may be faxed directly to the examiner at 571-273-4119, or sent via email at luke.wassum@uspto.gov, **with a previous written authorization in accordance with the provisions of MPEP § 502.03.** Such communications must be clearly marked as INFORMAL, DRAFT or UNOFFICIAL.

Customer Service for Tech Center 2100 can be reached during regular business hours at (571) 272-2100, or fax (571) 273-2100.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Luke S. Wassum/
Primary Examiner
Art Unit 2167

lsw
13 February 2009